(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 806 748 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.11.1997 Bulletin 1997/46

(51) Int Cl.[6]: G07F 7/12

(21) Application number: 97630024.4

(22) Date of filing: 06.05.1997

(84) Designated Contracting States:
DE FR GB

(30) Priority: 08.05.1996 JP 137580/96

(71) Applicants:
- Matsumoto, Tsutomu
  Sagamihara-shi, Kanagawa-ken (JP)
- NHK SPRING CO.LTD.
  Yokohama-shi, Kanagawa-ken (JP)

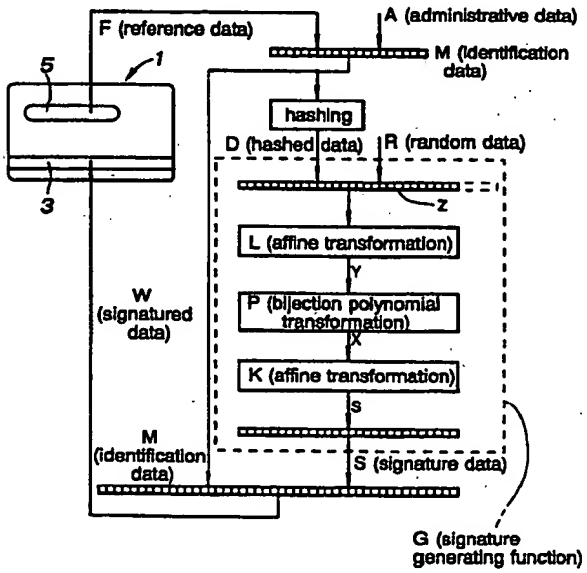
(72) Inventors:
- Ohno, Masatake, c/o NHK SPRING CO.,LTD.
  Yokohama-shi, Kanagawa-ken (JP)
- Matsumoto, Hiroyuki, c/o NHK SPRING CO.,LTD.
  Yokohama-shi, Kanagawa-ken (JP)
- Matsumoto, Tsutomu,
  Kanagawa-ken (JP)

(74) Representative: Schmitz, Jean-Marie et al
Dennemeyer & Associates S.A.,
P.O. Box 1502
1015 Luxembourg (LU)

(54) Security system based on certification

(57) The data containing reference data is transformed into signature data by a method which depends on a variable generated by the reference data, and the identification data is certified by inverse transformation of the signature data. The signature generating rule changes in dependence on the reference data, and it is therefore extremely difficult to analyze the signature generating rule from the medium or the card reader/writer so that the forgery or modification of magnetic or other data, which is otherwise easy to duplicate, can be made extremely difficult. Therefore, even when a reader is illicitly obtained, and analyzed, it is extremely difficult to estimate the signature generating rule as it owes to the difficulty of solving a set of multivariate simultaneous equations.

Fig. 3



EP 0 806 748 A2

Description

TECHNICAL FIELD

The present invention relates to a security system for preventing forgery and duplication of an object, such as a prepaid card, a credit card and an ID card, whose authenticity is required to be determined.

BACKGROUND OF THE INVENTION

As a means for preventing forgery or illicit duplication of an object, it has been proposed, for instance, to record a unique physical property of the object as data in advance, and to match the recorded data with the actual physical property of the object when the authenticity of the object is required to be verified. However, this cannot entire prevent an illicit duplication of the object by analyzing the physical property and duplicating the physical property.

According to a conventional security system, signature data is generated from original data by using a signature generating rule, and the authenticity of the original data is determined by verifying the signature data by using a signature verifying rule. The person who knows the signature verifying rule can verify the authenticity of the original data by verifying the signature data. Also, only the person who knows the signature generating rule can create his own signatured data, and change it. Because this system allows the authenticity of the data to be determined in an effective manner, there have been some attempts to affix a recording medium of the data in the form of a seal onto an object as a proof of the authenticity of the object.

However, even this system cannot totally prevent an attempt to forge the data by illicitly obtaining samples of signatured data and original data, and analyzing the data so as to decipher the signature generating rule and newly create signatured data.

BRIEF SUMMARY OF THE INVENTION

In view of such problems of the prior art, a primary object of the present invention is to provide a highly secure security system which can effectively prevent any forgery and duplication of an object.

A second object of the present invention is to provide a security system is highly secure against any attempt to break it but does not require a large number of data bits for its implementation.

A third object of the present invention is to provide a highly secure security system which does not require any large processing load.

A fourth object of the present invention is to provide a highly secure security system which can be economically implemented.

According to the present invention, such objects can be accomplished by providing a security system for preventing forgery or duplication of an object whose authenticity is required to be determined, comprising: a reference region affixed to an object, the reference region including a physical marking which is machine readable and is so randomly formed as to prevent any duplication thereof; an identification data storage region for retaining identification data which is based on reference data read from the reference region; and a signature data storage region for storing signature data for certifying the identification data; wherein the signature data is generated from the reference data and/or the identification data; and the authenticity of the object is determined according to a result of comparing the reference data read from the reference region with the reference data contained in the identification data and/or the signature data, and a result of certifying the identification data with the signature data, or by providing a security system for preventing forgery or duplication of an object whose authenticity is required to be determined, comprising: an identification data storage region for retaining identification data which is associated with a reference data, the reference data being individually assigned when writing the identification data into the identification data storage region; and a signature data storage region for storing signature data for certifying the identification data; wherein the signature data is generated by transforming data including the identification data and/or the reference data by using a variable which is generated from the identification data and/or the reference data; and the authenticity of the object is determined according to a result of certifying the identification data with data generated by inverse transformation of the signature data in a manner which corresponds to a variable generated from the identification data and/or the reference data.

The authenticity of the identification data stored in the identification data storage region is determined according to the reference data which is either arbitrarily selected or machine readable from a reference region, the reference region being formed so as to be difficult to be synthetically reproduced, and the identification data which is to be matched with the reference data, and solely by the signature data which is generated by a process dictated by the variable generated from the reference data. Therefore, even when a plurality of samples are made available, because the signature generating rule is different from one sample to another, analysis of the signature generating rule is extremely difficult, and without the knowledge of the signature generating rule for each sample, it is also difficult to newly create the signatured data or to modify it. Even when the signatured data is simply duplicated, because the reference data may vary from one object to another, its authenticity can be readily disproved, and any attempt to attach duplicated signature data to an illicit object pass off the illicit object for an authentic object can be readily detected.

In particular, when the authenticity of the object is determined according to a result of matching the data

read from the reference region during the course of the determination process with the reference data included in the identification data or the signature data, and a result of certifying the identification data, it is possible to detect an attempt copy the entire object carrying the signatured data because the level of agreement between the data read from the identification region during the course of the determination process with the reference data is low. In other words, the present invention can also effectively prevent simple copying of one object to another for illicit purpose.

Further, when the identification data consists of a combination of administrative data for managing the object and the reference data, it is possible to even more effectively prevent any illicit attempt to newly create signature data or to modify the data by separately comparing the administrative data with information associated with the object and the party which generated the signature.

When the signature data is generated from a compressed identification data obtained by data compressing the identification data, it is possible to reduce the bit length which is required to be processed, and to thereby reduce the time required for the signature verification.

The reference region may be formed by randomly placing magnetic fibers in paper or synthetic resin material or by utilizing an unevenness in paper, surface irregularities of sheet material or other machine readable but synthetically unreproduceable region. Such technologies are disclosed in United States Patents Nos. 4,218,674 and 4,734,695, and Japanese patent laid-open publication (kokai) No. 6-168363. The contents of these prior patents are hereby incorporated in this application by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

Now the present invention is described in the following with reference to the appended drawings, in which:

Figure 1 is a front view of a prepaid card which is given as an exemplary object to which the present invention is applied;

Figure 2 is a diagram showing an example of the card reader for the prepaid card;

Figure 3 is a block diagram showing the procedure for making a card according to a first embodiment of the present invention;

Figure 4 is a block diagram showing the details of the hashing process shown in Figure 3;

Figure 5 is a block diagram showing the procedure for certifying and reading a card according to the first embodiment of the present invention;

Figure 6 is a view similar to Figure 3 showing the procedure for making a card according to a second embodiment of the present invention; and

Figure 7 is a view similar to Figure 5 showing the procedure for certifying and reading a card according to the second embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows a prepaid card to which the present invention is applied. This card 1 consists of a polyester sheet 2, and carries thereon a magnetic stripe 3 which includes a storage region for storing identification data, the identification data being generated by combining administrative data, which specifies the issuing party, the kind of the card and the purpose of the card, with reference data which is described hereinafter, a perforation region 4 which is perforated as the card is spent, and a reference region 5 which is formed by randomly dispersing magnetic fibers in the resin material of the base sheet 2. The magnetic stripe 3 further includes a signature data storage region which is described hereinafter. Figure 2 shows a card reader to which the present invention is applied. The card reader 10 is incorporated with a card conveying unit 12 which includes motor-actuated rollers for taking a card into a slot 11, and ejecting the card 1 therefrom after the data is read. Along the length of the slot 11 are provided a magnetic head 13 for reading data from the magnetic stripe 3 and an induction magnetic head 14 for reading data from the reference region 5. Numeral 15 denotes a perforation unit for perforating the perforation region 4 of the card 1 to indicate how far the card is spent, and to destroy the reference region 5 as required.

The procedure for generating signature data in the card 1 or the procedure for preparing the card is described in the following with reference to Figure 3. First of all, a signal is read from the reference region 5 along a reading path defined by the card reader as reference data F, and it is combined with the administrative data A. The combined data is written into an identification data storage region of the magnetic stripe 3 as identification data M consisting of four 64-bit data blocks m1 to m4. Then, a hashing process as indicated in Figure 4 is applied to the identification data M. More specifically, data block m1 is combined with fixed 64-bit data blocks h0 and h0' to generate a pair of 64-bit data blocks h1 and h1'. Data block m2 is combined with the fixed data blocks h1 and h1' to generate a pair of 64-bit data blocks h2 and h2'. This process is repeated four times until a pair of 64-bit data blocks h4 and h4' are obtained. The finally obtained hashed data D has a 128-bit data length.

The hashed data D is combined with prescribed random data R as indicated in Figure 3 to generate input data Z having a bit length of 100 bits for instance, which is matched with the signature data to be written. An affine transformation L, a bijection polynomial transformation P, and an affine transformation K are successively carried out on the hashed data Z ($Z \rightarrow Y \rightarrow X \rightarrow S$) or, in other words, an arithmetic operation based on a signa-

ture generating function G is carried out to obtain final signature data S. The signature data S and the aforementioned identification data M are then written into the corresponding storage regions of the magnetic stripe 3. It is understood that the data which is written into the magnetic stripe is called as signatured data W. The signature data storage region and the identification storage region may be arranged separately from each other, but may store the data after it is ciphered and combined with each other by suitable ciphering means not shown in the drawings.

The bijection polynomial transformation P transforms an arbitrary element Y of a finite field into a certain element X, and the difficulty in analyzing the signature generating rule owes to the difficulty in solving a set of multivariate simultaneous equations. To further increase the difficulty in estimating signature generating function G from signature verifying function V which is described hereinafter, an affine transformation is carried out before and after the bijection polynomial transformation. The constants h0 and h0' for the hashing process may consist of arbitrary constants.

Arbitrary constants may also be selected for the affine transformations L and K and the bijection polynomial transformation P which are applied to the signature generating function G, but in the present embodiment, these constants are selected and modified according to a unique variable generated from the reference data F. Because the constants h0 and h0' as well as the constants for the affine transformations L and K and the bijection polynomial transformation P associated with the signature generating function can be arbitrarily selected, it is possible to a certification system in any one of a large number of possible ways, and the signature generating rule can be made harder to estimate all the more. In particular, by intervening random data in the process of signature generation, the estimation of the signature generating data can be made even more difficult in an effective manner.

When this card 1 is to be used, as shown in Figure 5, first of all, the identification data M' in the signatured data W' is hashed in a similar fashion to produce hashed data D'. At the same time, the signature data S' in the signatured data W' is inverse transformed by a multivariate polynomial-tuples (reverse of the $Z \rightarrow Y \rightarrow X \rightarrow S$ transformation) or, in other words, by an arithmetic operation using a signature verifying function V. The data obtained by the inverse transformation using the multivariate polynomial-tuples is separated into hashed data D* and random data R'. The signature is then verified by comparing the two sets of hashed data D' and D* to determine the authenticity of the original data.

At the same time, the identification data M' is separated int o reference data F' and administrative data A'. The reference data F' is compared with the reference data F* obtained from the identification region by the induction magnetic head 14, and the authenticity of the card is determined. data is verified by this signature verifying process. Only when the results of comparison between the two sets of hashed data D' and D* and between the two sets of reference data F' and F* are both satisfactory or only when the authenticity of the card is determined, a good signal is produced from the determining unit, and a prescribed service for each particular application is offered. It is also possible to produce a good signal when the administrative data A' matches with the administrative data A which was initially stored in means not shown in the drawings.

Because the duplication of the reference region is practically impossible, the duplication of the entire card can be avoided. The reference data F* which is read by the induction magnetic head 14 from the reference region can vary every time it is read because some positional errors are inevitable when conveying and stopping the card, the card may be soiled in different levels, and the magnetic state of the reference region normally changes with time. Therefore, in reality, the authenticity of the card may be verified when an agreement better than a certain tolerance level is established, instead of requiring an exact agreement. For instance, when an attempt is made to extract the reference data F' from the identification data M' stored as magnetic data, and read the reference data F* from the reference region 5 to compare them and analyze the relationship between them for illicit purpose, because the reference data F* changes every time it is read, it is quite impossible to analyze the relationship between the two sets of reference data F' and F* even when a number of samples are obtained. Thus, it is virtually impossible to make a card having an arbitrarily selected reference region, and to fabricate identification data M' which corresponds to the reference data obtained from the reference region. Furthermore, as it is extremely difficult to generate signature data from the identification data as mentioned above, modification of the data is also extremely difficult. Thus, copying of the entire card (article), forging (duplication) of the card, modification of data are all extremely difficult to carry out so that any illicit attempt on the object can be effectively prevented.

Figure 6 is a view similar to Figure 3 showing a second embodiment of the present invention. The basic structures of the prepaid card and the card reader are similar to those of the previous embodiment.

Referring to Figure 6, when making a card, first of all, a signal is read from the reference region 5 along a reading path defined by using a machine such as the card reader as reference data F, which is then combined with the administrative data A. The combined data is written into an identification data storage region of the magnetic stripe 3 as identification data M consisting of four 64-bit data blocks m1 to m4. Then, a hashing process such as the one described earlier with reference to Figure 4 is applied to the identification data M. This finally results in hashed data D which is 128-bit long.

The hashed data D is combined with prescribed random data R as indicated in Figure 6 to generate input

data Z having a bit length of 100 bits for instance, which is matched with the signature data to be written. An affine transformation L, a bijection polynomial transformation P, and an affine transformation K are successively carried out on the hashed data Z (Z→Y→X→S) or, in other words, an arithmetic operation based on a signature generating function G is carried out to obtain final signature data S. The signature data S and the aforementioned identification data M are then written into the corresponding storage regions of the magnetic stripe 3. It is understood that the data which is written into the magnetic stripe is called as signatured data W. The signature data storage region and the identification storage region may be arranged separately from each other, but may store the data after it is ciphered and combined with each other by suitable ciphering means not shown in the drawings.

The bijection polynomial transformation P transforms an arbitrary element Y of a finite field into a certain element X, and the difficulty in analyzing the signature generating rule owes to the difficulty in solving a set of multivariate simultaneous equations. To further increase the difficulty in estimating signature generating function G from signature verifying function V, an affine transformation is carried out before and after the bijection polynomial transformation. The constants h0 and h0' for the hashing process may consist of arbitrary constants.

Arbitrary constants may also be selected for the affine transformations L and K and the bijection polynomial transformation P which are applied to the signature generating function G, but in the present embodiment, these constants are selected and modified according to a unique variable u generated from the reference data F. This may be accomplished by looking up a table defining a relationship between the variable u and the constants. It is also possible to define a function which generates the constants from the selected variable. In practice, it is also possible to change the transformation algorithm itself for the bijection polynomial transformation P according to the variable u. It is thus possible to form a highly adaptable certification system and to make the estimation of the signature generating rule extremely difficult. In particular, by intervening random data in the process of signature generation, the estimation of the signature generating data can be made even more difficult in an effective manner.

When this card 1 is to be used, as shown in Figure 7, first of all, the identification data M' in the signatured data W' is separated into reference data F' and administrative data A'. The reference data F' is compared with reference data F* obtained by the induction magnetic head 14 from the reference region 5 to verify the authenticity of the card 1. When the authenticity of the card is verified, the hashing process is applied to the identification data M' in a similar manner to produce hashed data D'. At the same time, the signature data S' in the signatured data W' is inverse transformed by a multivariate polynomial- tuples (reverse of the Z→Y→X→S transformation) or, in other words, by an arithmetic operation using a signature verifying function V. At this point, variable u' is generated from the reference data F' in a similar fashion to obtain the constant for the multivariate polynomial- tuples or the inverse transformation algorithm. The data obtained by the inverse transformation using the multivariate polynomial- tuples is separated into hashed data D* and random data R'. The signature is then verified by comparing the two sets of hashed data D' and D* to determine the authenticity of the original data. Only when the verification process is completed in a normal manner or the authenticity of the card is verified, a good signal is produced from the determining unit to permit offering of services for each particular application. It is also possible to produce a good signal when the administrative data A' matches with the administrative data A which was initially stored in means not shown in the drawings.

The reference region 5 was formed by randomly dispersing magnetic fibers in the resin material of the base sheet 2 in the above described second embodiment, but it is also possible to simply form a bar code for recording the variable u. If the cycle of recording and reading is conducted in a relatively short period of time, it is also possible to set reference data on the reader/writer, instead of forming a reference region on the object, and change the reference data either regularly or irregularly.

It is also possible to allow the relationship between the variable u and the constants to be manipulated from outside as illustrated in Figures 6 and 7. For instance, the table for associating the variable u with the constants or the mathematical function for generating the constants from the variable u may be adapted to be modified from outside. The same is true with the arrangement for changing the transformation algorithm of the bijection polynomial transformation itself according to the variable u.

The object consisted of an information storage card or an ID card in the above described embodiments, but it is obvious for a person skilled in the art that the present invention can be applied to jewelry, security notes, and keys to rooms and vehicles which have known values, and are required to be verified of their authenticity.

Thus, according to the present invention, a highly complex certification system can be achieved by using signature data consisting of a relatively small bit length. Furthermore, the processing time required for signature generation and signature verification is not increased, and the sizes of the program and the memory required for executing the algorithm are no more than what can be readily incorporated in a conventional card reader/writer without any problem.

In particular when the identification data is matched with the reference data read from a region which cannot be easily reproduced or duplicated, it is extremely difficult to illicitly duplicate the object such as an information storage card. Also, it is extremely difficult to analyze the

system from a number of samples of the object.

It is also difficult to analyze the signature generating rule from the card or the card reader. In other words, even when a card reader is obtained, and is analyzed, it still is extremely difficult to estimate the signature generating rule because the difficulty owes to the difficulty in solving a set of multivariate simultaneous equations.

The data containing the reference data is transformed into the signature data by a method which depends on a variable generated by the reference data, and the identification data is certified by inverse transformation of the signature data. The signature generating rule changes in dependence on the reference data (or a variable generated thereby), and it is therefore extremely difficult to analyze the signature generating rule from the medium (object) or the card reader/writer so that the forgery or modification of the magnetic data, which is otherwise easy to duplicate, can be made extremely difficult. Therefore, even when a reader (signature verifier) is illicitly obtained, and analyzed, it is extremely difficult to estimate the signature generating rule as it owes to the difficulty of solving a set of multivariate simultaneous equations. Furthermore, because the signature generating rule changes for each particular reference data (For instance, if the object has its own unique reference data, the signature generating rule changes for each object.), the analysis of the reference data is so difficult that any attempt to generate or modify signatured data can be effectively prevented.

Furthermore, by using reference data which is obtained from a non-reproduceable reference region, and requiring the matching between the reference data read from the reference region with the signatured identification data when determining the authenticity of the article, any illicit attempt to duplicate the object or the card will be made extremely difficult. Likewise, analyzing the system from a plurality of card samples is also extremely difficult to accomplish.

Although the present invention has been described in terms of preferred embodiments thereof, it is obvious to a person skilled in the art that various alterations and modifications are possible without departing from the scope of the present invention which is set forth in the appended claims.

Claims

1. A security system for preventing forgery or duplication of an object whose authenticity is required to be determined, comprising:

   a reference region affixed to an object, said reference region including a physical marking which is machine readable and is so randomly formed as to prevent any duplication thereof;
   an identification data storage region for retaining identification data which is based on reference data read from said reference region; and
   a signature data storage region for storing signature data for certifying said identification data;
   wherein said signature data is generated from said reference data and/or said identification data; and
   the authenticity of said object is determined according to a result of comparing said reference data read from said reference region with said reference data contained in said identification data and/or said signature data, and a result of certifying said identification data with said signature data.

2. A security system based on certification according to claim 1, wherein said identification data consists of a combination of administrative data for managing said object and said reference data.

3. A security system based on certification according to claim 1, wherein said signature data is generated from a compressed identification data obtained by data compressing said identification data.

4. A security system based on certification according to claim 1, wherein said reference region is formed by randomly placing magnetic fibers in paper and/or synthetic resin material.

5. A security system for preventing forgery or duplication of an object whose authenticity is required to be determined, comprising:

   an identification data storage region for retaining identification data which is associated with a reference data, said reference data being individually assigned when writing said identification data into said identification data storage region; and
   a signature data storage region for storing signature data for certifying said identification data;
   wherein said signature data is generated by transforming data including said identification data and/or said reference data by using a first variable which is generated from said identification data and/or said reference data; and
   the authenticity of said object is determined according to a result of certifying said identification data with data generated by inverse transformation of said signature data in a manner which corresponds to a second variable generated from said identification data and/or said reference data.

6. A security system based on certification according to claim 5, wherein said reference data is generated

by reading data from a reference region which is affixed to said object and is machine readable, said identification region being formed in such a physically random fashion as to make any duplication of said identification region extremely difficult.

7. A security system based on certification according to claim 5, wherein the authenticity of said object is determined according to a result of matching said reference data read from said reference region during the course of an authenticity determination process with said reference data included in said identification data and/or said signature data, and a result of certifying said identification data with said data generated by inverse transformation of said signature data in a manner which corresponds to a second variable generated from said identification data and/or said reference data.

8. A security system based on certification according to claim 5, wherein said identification data consists of a combination of administrative data for managing said object and said reference data.

9. A security system based on certification according to any claim 5, wherein said signature data is generated from a compressed identification data obtained by data compressing said identification data.

10. A security system based on certification according to claim 5, wherein said reference region is formed by randomly placing magnetic fibers in paper or synthetic resin material.

11. A security system based on certification according to claim 5, wherein said first variable is related to a constant of said transformation.

12. A security system based on certification according to claim 5, wherein said first variable is related to an algorithm for said transformation.

13. A security system based on certification according to claim 5, wherein said transformation comprises a bijection polynomial transformation.

14. A security system based on certification according to claim 5, wherein said transformation further comprises an affine transformation.

15. A security system based on certification according to claim 1, wherein said transformation comprises a bijection polynomial transformation.

16. A security system based on certification according to claim 1, wherein said transformation further comprises an affine transformation.

Fig. 1

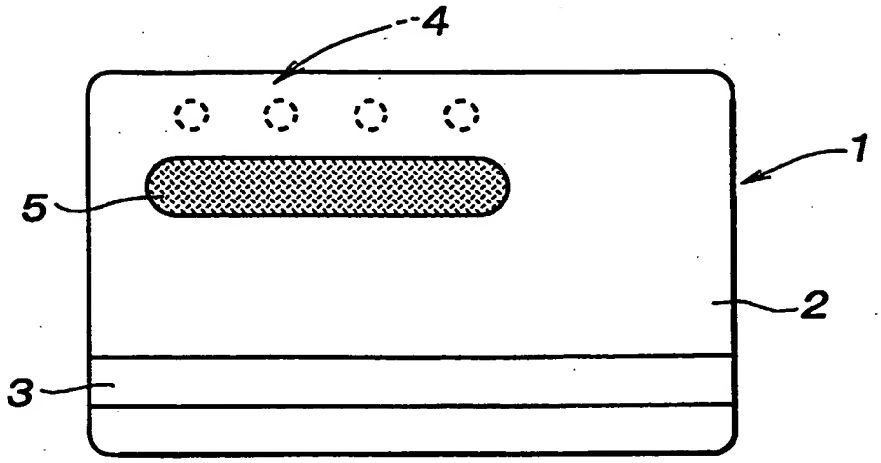


Fig. 2

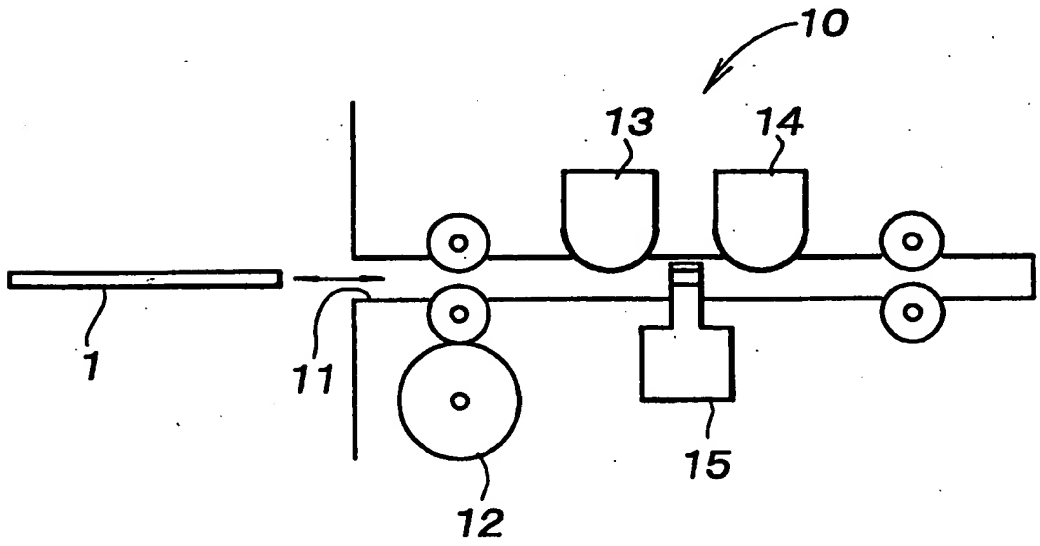


Fig. 3

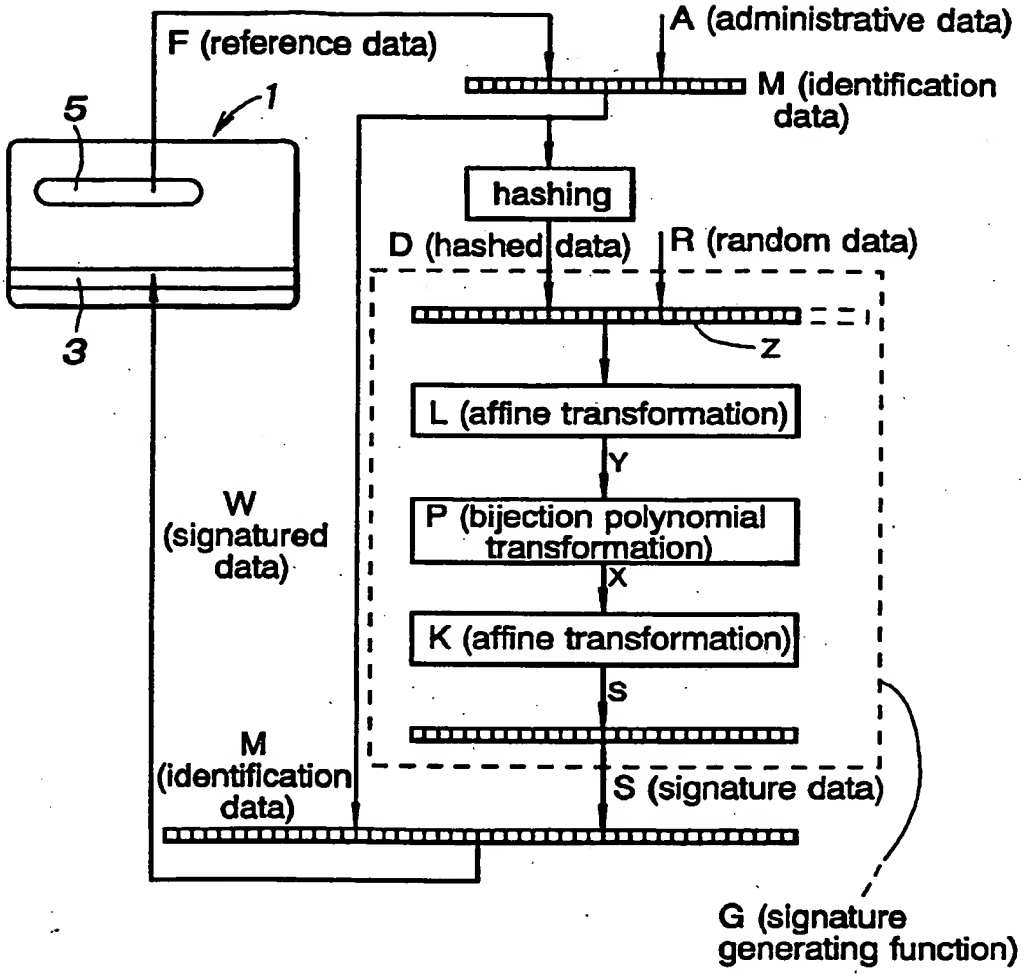

F (reference data)
A (administrative data)
M (identification data)
5
1
3
hashing
D (hashed data)
R (random data)
Z
L (affine transformation)
Y
W (signatured data)
P (bijection polynomial transformation)
X
K (affine transformation)
S
M (identification data)
S (signature data)
G (signature generating function)

Fig. 4

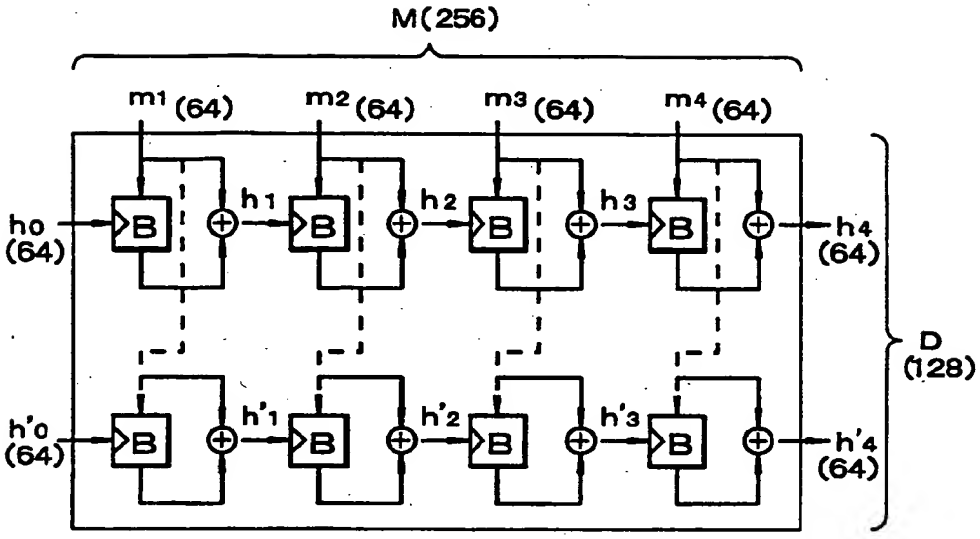

M(256)
m1 (64)
m2 (64)
m3 (64)
m4 (64)
h0 (64)
h1
h2
h3
h4 (64)
h'0 (64)
h'1
h'2
h'3
h'4 (64)
B
D (128)

Fig. 5

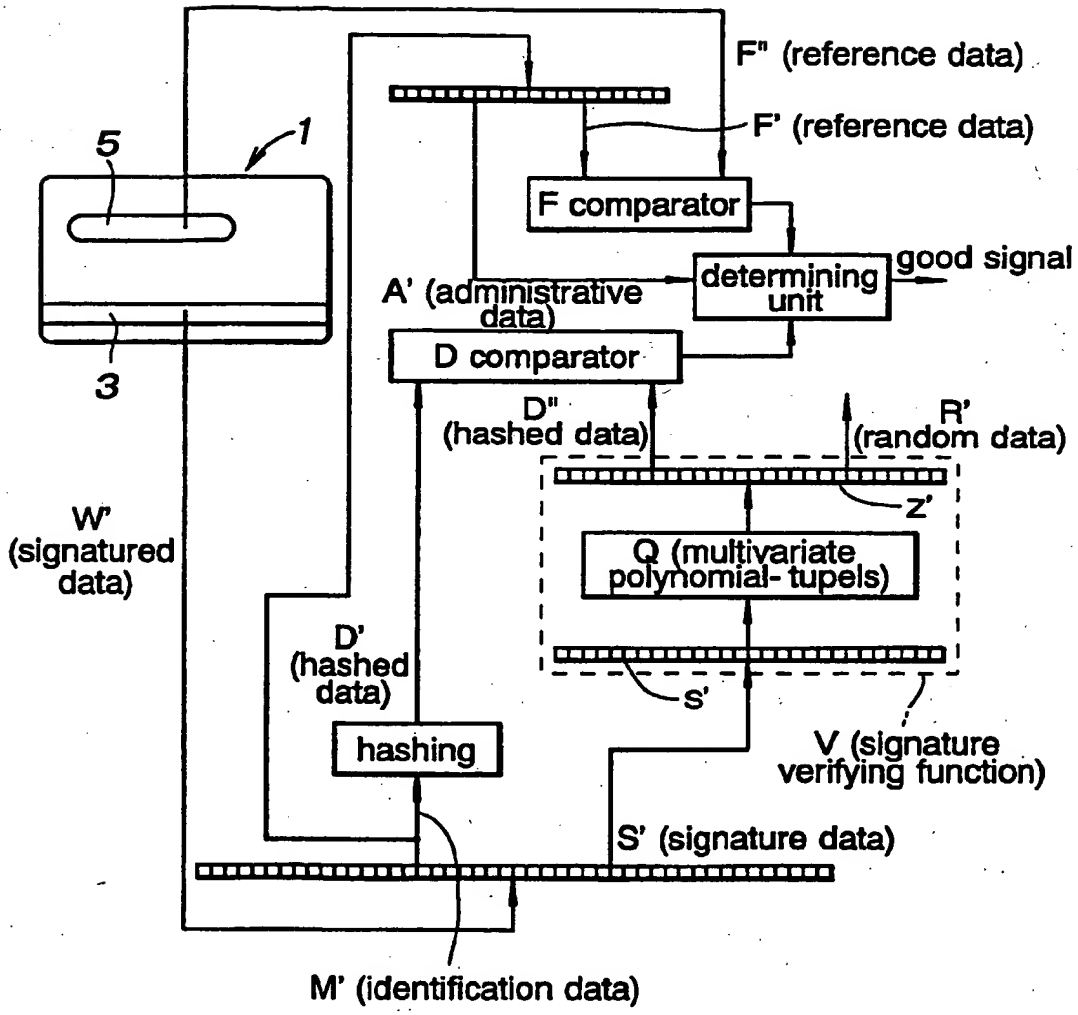

F" (reference data)
F' (reference data)
5
1
F comparator
determining unit
good signal
A' (administrative data)
D comparator
3
D"
(hashed data)
R'
(random data)
W'
(signatured data)
Z'
Q (multivariate polynomial- tupels)
D'
(hashed data)
S'
hashing
V (signature verifying function)
S' (signature data)
M' (identification data)

Fig. 6

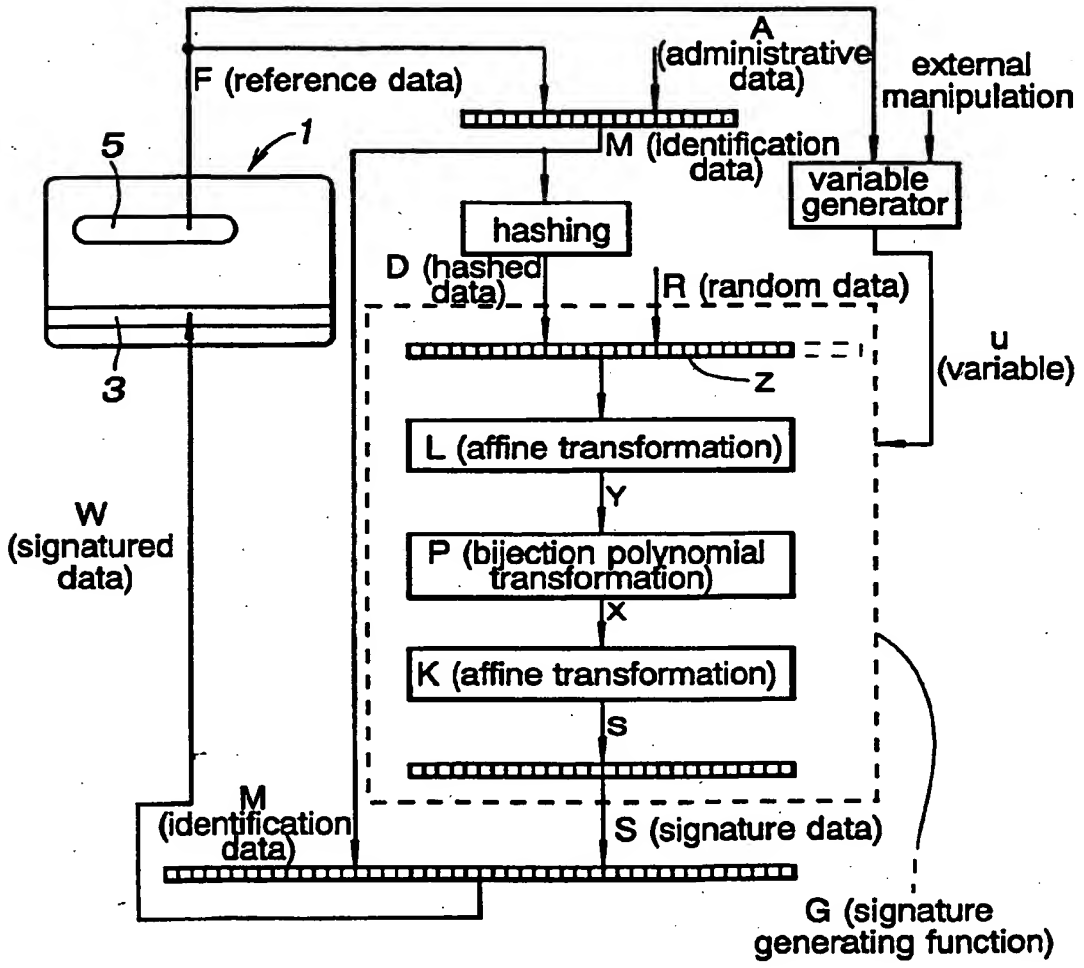
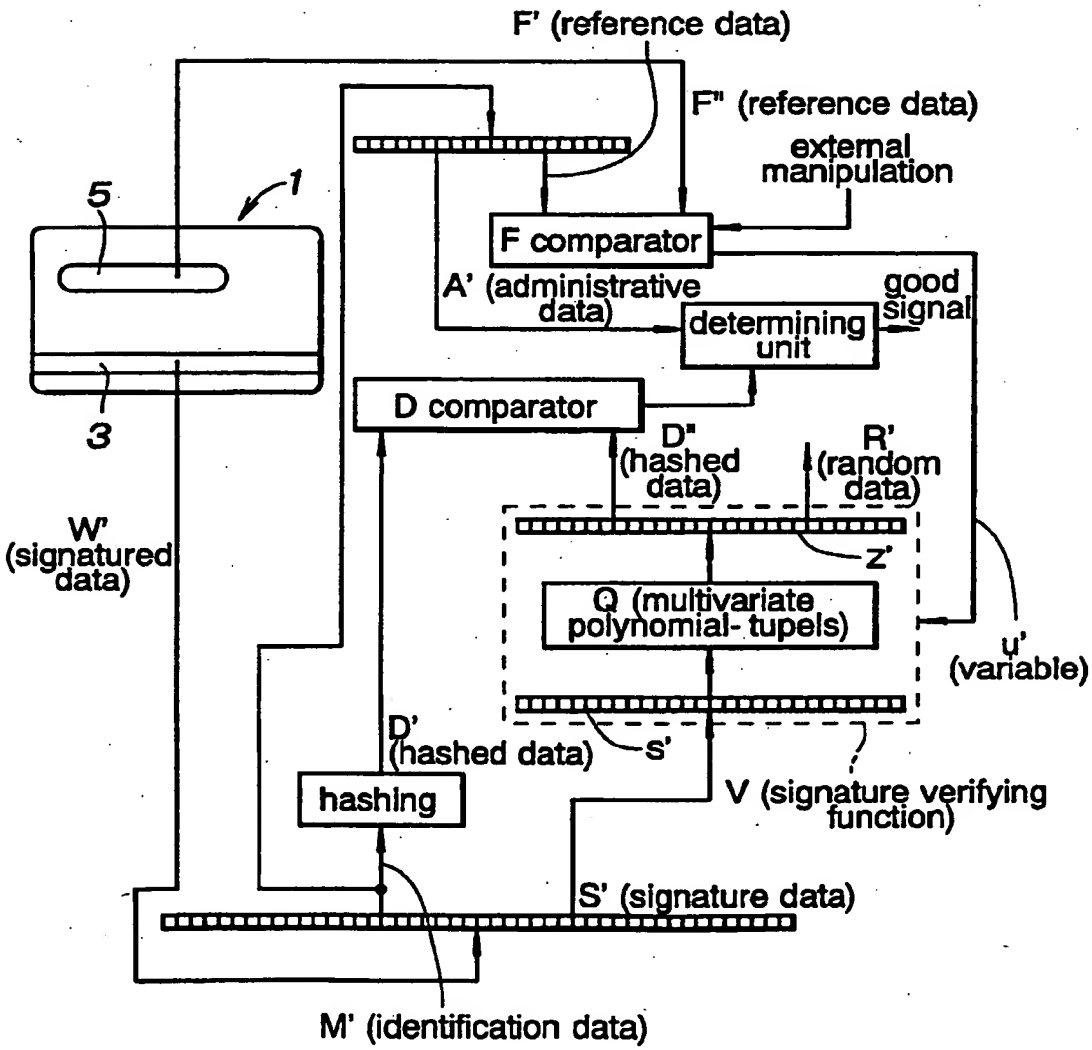

A
(administrative data)
external manipulation
F (reference data)
5
1
M (identification data)
variable generator
hashing
D (hashed data)
R (random data)
u
(variable)
3
z
L (affine transformation)
Y
W
(signatured data)
P (bijection polynomial transformation)
X
K (affine transformation)
S
M
(identification data)
S (signature data)
G (signature generating function)

Fig. 7


F' (reference data)
F" (reference data)
external manipulation
5
1
F comparator
A' (administrative data)
good signal
determining unit
D comparator
3
D" (hashed data)
R' (random data)
W' (signatured data)
z'
Q (multivariate polynomial-tupels)
u' (variable)
D' (hashed data)
s'
V (signature verifying function)
hashing
S' (signature data)
M' (identification data)